(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－212089

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｂ
			7259－5Ｊ			６３０Ｅ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｄ
						６０１Ｆ

審査請求　未請求　請求項の数31　ＯＬ　（全 16 頁）

(21)出願番号　特願平8－18541

(22)出願日　平成８年(1996)２月５日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　滝本　智之　（外１名）

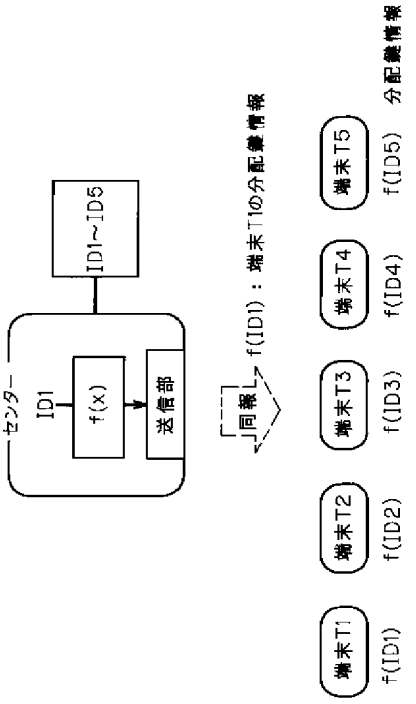
最終頁に続く

(54)【発明の名称】　鍵共有装置

(57)【要約】

【課題】　特定端末だけを排除して、残りの端末で秘密鍵を共有する。

【解決手段】　公知の(k,n)しきい値法の手法を上記課題解決の為に新たに適用する。(1) 各端末IDiは１次多項式f(x)で定められる(k,n)しきい値法の各分配鍵情報f(IDi)を保持。各端末の分配鍵情報は１つだけでよい。(2) 端末T1を排除する場合、センターは端末T1の分配鍵情報f(ID1)を同報で全端末に通知（図２）。１端末だけを排除する場合センターは１つの分配鍵情報を同報で通知するだけでよい。(3) 端末T1以外の端末では1)で保持している自分の分配鍵情報と(2)で通知された情報を用いて１次多項式f(x)を求める。(4) 端末T1だけは(1)と(2)の情報が一致するため、１次多項式を求めることができない。



【特許請求の範囲】

【請求項１】センターと相異なる分配鍵情報を持つ複数の端末からなり、センターは全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、kを正整数とするとき、特定のk個の端末の分配鍵情報を同報で全端末に通知する通知部を備え、各端末は、分配鍵情報を格納する分配鍵情報格納部と、前記センターから通知されたk個の分配鍵情報を受信する受信部と、前記受信部で受信したk個の分配鍵情報と、前記分配鍵情報格納部に格納される分配鍵情報の計k+1個の分配鍵情報がすべて相異なる場合にのみ、これらk+1個の分配鍵情報より前記特定のk個の端末を除く残りの端末で共通の秘密鍵を算出する秘密鍵算出部からなり、前記各端末の分配鍵情報は、前記秘密鍵算出部に入力されるk+1個の分配鍵情報がすべて相異なる場合にのみ前記秘密鍵が復元できるように予め定められ各端末に分配されたものであることを特徴とする鍵共有装置。

【請求項２】前記センターが、全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、前記全端末の分配鍵情報以外の予備の分配鍵情報を格納する予備分配鍵情報格納部と、kとmをそれぞれ正整数とするとき、特定のm個の端末の分配鍵情報と任意のk-m個の予備分配鍵情報の合計k個の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする請求項１記載の鍵共有装置。

【請求項３】前記センターが、前記全端末の分配鍵情報以外の予備の分配鍵情報を格納する予備分配鍵情報格納部と、任意のk個の予備の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする請求項１記載の鍵共有装置。

【請求項４】前記各端末は相異なる識別情報を保持し、前記センターは全端末分配鍵情報格納部の代わりに、前記秘密鍵を保持する秘密鍵格納部と、前記秘密鍵と任意の端末の識別情報を入力として、対応する端末の分配鍵情報を算出する分配鍵情報算出部を備えていることを特徴とする請求項１記載の鍵共有装置。

【請求項５】前記各端末は相異なる識別情報を保持し、前記センターは前記予備分配鍵情報格納部の代わりに、前記秘密鍵を保持する秘密鍵格納部と、どの端末の識別情報とも異なる予備の情報と前記秘密鍵を入力として、前記予備の分配鍵情報を算出する予備分配鍵情報算出部を備えていることを特徴とする請求項２または請求項３記載の鍵共有装置。

【請求項６】センターと相異なる分配鍵情報を持つ複数の端末からなり、センターは全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、kを正整数とするとき、特定のk個の端末の分配鍵情報を同報で全端末に通知する通知部を備え、各端末は、分配鍵情報を格納する分配鍵情報格納部と、前記センターから通知されたk個の分配鍵情報を受信する受信部と、前記受信部で受信したk個の分配鍵情報と、前記分配鍵情報格納部に格納される分配鍵情報の計k+1個の分配鍵情報がすべて相異なる場合にのみ、これらk+1個の分配鍵情報より前記特定のk個の端末を除く残りの端末で共通の第１の秘密鍵を算出する秘密鍵算出部と、前記第１の秘密鍵を全端末共通の変換方法で変換して第２の秘密鍵を求める変換部と、前記第２の秘密鍵から端末の新しい分配鍵情報を算出し、前記分配鍵情報格納部に格納して分配鍵情報を更新する分配鍵情報更新部からなり、前記各端末の更新前の分配鍵情報は、前記秘密鍵算出部において入力されるk+1個の分配鍵情報がすべて相異なる場合にのみ前記第１の秘密鍵が復元できるように予め定められ各端末に分配されたものであり、前記分配鍵情報更新部によって更新された各端末の分配鍵情報は、前記と同様に前記第２の秘密鍵が復元できるように定められて各端末に分配されたものになり、前記各端末の変換部と分配鍵情報更新部は、外部より観察したり、変更できないものであり、前記センターの全端末分配鍵情報格納部は、前記各端末で更新された分配鍵情報を格納することを特徴とする鍵共有装置。

【請求項７】前記変換部と分配鍵情報更新部を外部より観察したり、変更できない領域に備える代わりに、分配鍵情報更新部が、分配鍵情報を更新した後に前記第２の秘密鍵を消去することを特徴とする請求項６記載の鍵共有装置。

【請求項８】前記センターが、全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、前記全端末の分配鍵情報以外の予備の分配鍵情報を格納する予備分配鍵情報格納部と、kとmをそれぞれ正整数とするとき、特定のm個の端末の分配鍵情報と任意のk-m個の予備分配鍵情報の合計k個の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする請求項６記載の鍵共有装置。

【請求項９】前記センターが、前記全端末の分配鍵情報以外の予備の分配鍵情報を格納する予備分配鍵情報格納部と、任意のk個の予備の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする請求項６記載の鍵共有装置。

【請求項１０】前記センターは前記全端末分配鍵情報格納部の代わりに、前記第１の秘密鍵を保持する秘密鍵格納部と、前記第１の秘密鍵と任意の端末の識別情報を入力として、対応する端末の分配鍵情報を算出する分配鍵情報算出部と、前記第１の秘密鍵を各端末の変換部と同じ変換方法で変換して第２の秘密鍵を求め、前記秘密鍵格納部に格納して第１の秘密鍵を更新するセンター側変換部を備えることを特徴とする請求項６記載の鍵共有装置。

【請求項１１】前記センターは前記予備分配鍵情報格納部の代わりに、前記第１の秘密鍵を保持する秘密鍵格納部と、どの端末の識別情報とも異なる予備の情報と前記

第１の秘密鍵を入力として、前記予備の分配鍵情報を算出する予備分配鍵情報算出部と、前記第１の秘密鍵を各端末の変換部と同じ変換方法で変換して第２の秘密鍵を求め、前記秘密鍵格納部に格納して第１の秘密鍵を更新するセンター側変換部を備えることを特徴とする請求項８または請求項９記載の鍵共有装置。

【請求項１２】前記各端末内の変換部およびセンター側変換部において、固定の変換の代わりに、外部から変更できる変換を用いることを特徴とする請求項６～１１のいずれか１項に記載の鍵共有装置。

【請求項１３】前記各端末内の分配鍵情報更新部で、前記第２の秘密鍵と前記端末の識別情報を用いて、前記端末の新しい分配鍵情報を算出することを特徴とする請求項６～１１のいずれか１項に記載の鍵共有装置。

【請求項１４】前記各端末内の分配鍵情報更新部で、前記第２の秘密鍵と端末の更新前の分配鍵情報を用いて、前記端末の新しい分配鍵情報を算出することを特徴とする請求項６～９のいずれか１項に記載の鍵共有装置。

【請求項１５】センターと相異なる識別情報と分配鍵情報を持つ複数の端末からなり、kを正整数、pを素数とし、ak,ak-1,…,a1,a0をp未満の非負整数とするとき、識別情報IDiが与えられている端末の前記分配鍵情報は、法p上のk次多項式（数１）の座標(IDi,f(IDi))であり、

【数１】

$$f(x)=akxk+ak-1xk-1+\cdots+a1x+a0 \mod p$$

前記センターは全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、特定のk個の端末の分配鍵情報を同報で全端末に通知する通知部を備え、各端末は、分配鍵情報を格納する分配鍵情報格納部と、前記センターから通知されたk個の分配鍵情報を受信する受信部と、前記受信部で受信したk個の分配鍵情報と、前記分配鍵情報格納部に格納される分配鍵情報の計k+1個の分散鍵情報がすべて相異なる場合にのみ、これらk+1個の分配鍵情報である前記k次多項式の相異なるk+1個の座標から、前記k次多項式の１つ以上の係数を求めてそれらから秘密鍵を算出する秘密鍵算出部からなる鍵共有装置。

【請求項１６】前記センターが、全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、どの端末の識別情報とも異なる情報Xをx座標とする前記k次多項式の座標(X, f(X))を予備の分配鍵情報として格納する予備分配鍵情報格納部と、kとmをそれぞれ正整数とするとき、特定のm個の端末の分配鍵情報と任意のk-m個の予備分配鍵情報の合計k個の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする請求項１５記載の鍵共有装置。

【請求項１７】前記センターが、どの端末の識別情報とも異なる情報Xをx座標とする前記k次多項式の座標(X, f(X))を予備の分配鍵情報として格納する予備分配鍵情報格納部と、任意のk個の予備の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする請求項１５記載の鍵共有装置。

【請求項１８】前記センターは前記全端末分配鍵情報格納部または予備分配鍵情報格納部の代わりに、前記法p上のk次多項式を保持し、前記識別情報IDiが与えられている端末の分配鍵情報を、前記k次多項式に前記端末の識別情報を代入して求め、またどの端末の識別情報とも異なる情報を前記k次多項式に代入して前記予備分配鍵情報を求める分配鍵情報算出部を備えていることを特徴とする請求項１５～１７のいずれか１項に記載の鍵共有装置。

【請求項１９】センターと相異なる識別情報と分配鍵情報を持つ複数の端末からなり、kを正整数、pを素数とし、ak,ak-1,…,a1,a0をp未満の非負整数とするとき、識別情報IDiが与えられている端末の前記分配鍵情報は、法p上の第１のk次多項式（数１）の座標(IDi,f(IDi))であり、前記センターは全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、特定のk個の端末の分配鍵情報を同報で全端末に通知する通知部を備え、各端末は、分配鍵情報を格納する分配鍵情報格納部と、前記センターから通知されたk個の分配鍵情報を受信する受信部と、前記受信部で受信したk個の分配鍵情報と、前記分配鍵情報格納部に格納される分配鍵情報の計k+1の分配鍵情報がすべて相異なる場合にのみ、これらk+1個の分配鍵情報である前記第１のk次多項式の相異なるk+1個の座標から、前記第１のk次多項式のk+1個の係数を求める秘密鍵算出部と、前記第１のk次多項式f(x)の各係数を変換して第２のk次多項式g(x)を求める変換部と、前記第２のk次多項式の座標（IDi, g(IDi)）を求めてこれを新たな分配鍵情報として、前記分配鍵情報格納部に格納する分配鍵情報更新部からなり、前記各端末の変換部と分配鍵情報更新部は、外部より観察したり、変更できないものであり、前記センターの全端末分配鍵情報格納部では前記各端末で更新された分配鍵情報を格納することを特徴とする鍵共有装置。

【請求項２０】前記各端末の変換部と分配鍵情報更新部を外部より観察したり、変更できない領域に備える代わりに、分配鍵情報更新部が、分配鍵情報を更新した後に前記第２のk次多項式g(x)の各係数を消去することを特徴とする請求項１９記載の鍵共有装置。

【請求項２１】前記端末の変換部で、前記端末の識別情報を変換してその結果を新たな識別情報とし、前記分配鍵情報更新部ではこの新たな識別情報をx座標とする前記第２のk次多項式の座標を求めてこれを新たな分配鍵情報とすることを特徴とする請求項１９記載の鍵共有装置。

【請求項２２】前記センターは前記全端末分配鍵情報格納部の代わりに、前記第１のk次多項式を保持し、前記識別情報IDiが与えられている端末の分配鍵情報を、前記第１のk次多項式に前記端末の識別情報を代入して求

める分配鍵情報算出部と、前記第１のk次多項式f(x)のk+1個の係数を前記端末における変換部と同じ変換方法で変換して第２のk次多項式g(x)を求め、前記第１のk次多項式に置き換えてこれを保持するセンター側変換部を備えることを特徴とする請求項１９記載の鍵共有装置。

【請求項２３】mを正整数とし、jを1からmのそれぞれの値をとるときjを添字とする各pjを素数としてこれに対応して前記と同様に法pj上のk次多項式fj(x)をそれぞれ定め、識別情報IDiが与えられている端末の分配鍵情報を、各座標(IDi,f1(IDi))(IDi,f2(IDi)),…,(IDi,fm(IDi))で与えられるm個の情報とし、センターにおける通知部では、特定のk個の端末の各m個の分配鍵情報を同報で全端末に通知し、各端末における秘密鍵算出部では、jを1からmのそれぞれの値をとるとき、各jについて相異なるk+1個の分配鍵情報がそろった場合にのみ、これらk+1個の分配鍵情報である前記k次多項式fj(x)の相異なるk+1個の座標から前記k次多項式fjのk+1個の係数を求めることを特徴とする請求項１５～２２のいずれか１項に記載の鍵共有装置。

【請求項２４】センターと相異なる識別情報を持つ複数の端末からなり、k,mを正整数、jを1からmまでのそれぞれの値をとるとき、jを添字とする各pjを素数とし、aj,bjをpj未満の非負整数とするとき、識別情報IDiが与えられている端末の分配鍵情報を、法pj上の1次多項式（数２）の各座標(IDi,f1(IDi))(IDi,f2(IDi)),…,(IDi,fm(IDi))で与えられるm個の情報とし、

【数２】

$$fj(x)=aj\times x+bj \mod pj$$

センターにおける通知部では、特定の端末の保持する各m個の分配鍵情報から任意に選んで同報で全端末に通知し、各端末は、前記センターから通知された分配鍵情報を受信する受信部と、前記j番目の分配鍵情報を格納する合計m個の分配鍵情報格納部と、前記受信部で受信した分配鍵情報の中から前記jに対応した分配鍵情報を選び、これと前記j番目の分配鍵情報格納部に格納された分配鍵情報と合わせて相異なる2個の分配鍵情報がそろった場合にのみ相異なる2個の座標から前記1次多項式fj(x)の係数を求める、合計m個の秘密鍵算出部を備える請求項１５～２２のいずれか１項に記載の鍵共有装置。

【請求項２５】前記各jに対応するm個の多項式を、それぞれ1次以上の多項式とすることを特徴とする請求項２４記載の鍵共有装置。

【請求項２６】前記素数pまたは素数pjを法とする多項式の代わりに、素体の拡大体上の多項式とすることを特徴とする請求項１５～２２のいずれか１項に記載の鍵共有装置。

【請求項２７】前記秘密鍵算出部において、入力のk+1個の分配鍵情報に誤りが生じえる場合や、k+1個より多い分配鍵情報が入力された場合に、その中で正しいk+1個の相異なる分配鍵情報を用いて秘密鍵を算出することを特徴とする請求項１～２２のいずれか１項に記載の鍵共有装置。

【請求項２８】前記各端末の秘密鍵算出部で求める多項式の係数の一部、または前記係数を含んだ計算結果を特定のk個の端末を除く各端末の共通鍵とすることを特徴とする請求項１５～２６のいずれか１項に記載の鍵共有装置。

【請求項２９】前記センターは鍵データを発生し、これを前記共通鍵で暗号化した結果を、前記通信部で前記分配鍵情報とともに同報で全端末に通知し、前記特定のk個の端末を除く各端末では前記算出した共通鍵でこれを復号することを特徴とする請求項２８記載の鍵共有装置。

【請求項３０】前記秘密鍵にバージョン番号を付加し、センターは各バージョンの予備の分配鍵情報を保管し、バージョンが一致していない端末に前記必要な分配鍵情報を通知することを特徴とする請求項１～２６のいずれか１項に記載の鍵共有装置。

【請求項３１】前記秘密鍵にバージョン番号を付加し、バージョンが一致していない端末に正しいバージョンの秘密鍵を個別に暗号化して通知することを特徴とする請求項６～１４、および請求項１９～２２のいずれか１項に記載の鍵共有装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、センターおよび複数端末からなる通信システムにおいて暗号通信を行うシステムに関し、特にセンターから複数端末に共通の秘密鍵を安全に配送する装置に関する。さらにセンターからの通信量を削減してセンターが特定した端末以外のすべての端末で秘密鍵を共有する鍵共有装置に関するものである。

【０００２】

【従来の技術】センターおよび複数端末からなる通信システムにおいて、センターの管理のもと複数の端末がグループを形成し、グループで同じ秘密鍵を共有して同報の暗号通信を行う場合を考える。グループの秘密鍵を用いて暗号化された情報は、同じ秘密鍵を保有するグループ内の端末だけが復号することができる。ところで、このグループから特定の端末を排除したい場合が生じうる。それは例えばグループ内のある端末が盗難され、その端末を用いた暗号通信の盗聴や偽情報の送信などの不正が考えられる場合などである。このとき、この秘密鍵を管理するセンターは、できるだけ速やかに、盗難された端末を排除して、残りの端末だけで新たな秘密鍵を共有することが必要となる。

【０００３】（従来例１）図１１はセンターが特定した端末以外で鍵データを共有するための、第１の従来例における鍵共有方法である。この図では５個の端末T1,…,T5がそれぞれ固有の固有鍵k1,…,k5を保持しており、セ

ンターCは全端末の固有鍵を管理している。例えばセンターが端末T1を排除して他のT2,…,T5で新しい共通の秘密鍵を配付するためには、まず、センターは秘密鍵Kを生成し、これをそれぞれk2,…,k5を鍵として暗号化し、それぞれT2,…,T5に配送する。各端末では固有鍵を用いてこれを復号し、秘密鍵Kを獲得する。なお、図中において例えばEk2(K)はKを固有鍵k2で暗号化した暗号文である。この通信路上のデータはそれぞれ端末T2～T5の固有鍵で暗号化されているため、たとえ端末T1がこの通信データを盗聴したとしてもセンターが生成した分配鍵情報Kを獲得することができない。

【０００４】しかし、この方法では一般にN個の端末から１つの端末を排除するためには、センターはN-1回の暗号化を行い、N-1個のデータを送信しなくてはならない。グループが大きくなると、この作業はセンターにとって非常に負担になる。また、全局更新まではグループ内の暗号通信等の業務を停止する必要があるが、N-1局に配り終えるまでの業務停止期間が長いと大きな問題である。

【０００５】（従来例２）図１２に第２の従来例における鍵共有方法について示す。この方法では、従来例１における端末をグループ化して、センター側の暗号化の手間と送信データ量の削減を行う。この図では５つの端末をT1,T2と残りの３端末の、２つのグループに分けて、それぞれで共通のグループ鍵G1,G2を共有している。そして例えばセンターが端末T1を排除する場合には、端末T2に対しては生成した分配鍵情報KをT2の固有鍵k2を用いて暗号化し、残りのT3,T4,T5に対してはグループ鍵G2を用いて分配鍵情報Kを暗号化して配送する。T3,T4,T5の各端末ではそれぞれグループ鍵G2を用いてこれを復号し分配鍵情報Kを獲得する。なお、端末のグループ化は多重や階層的に行うことも考えられる。

【０００６】しかし、第２の従来例では各端末に固有の固有鍵に加えて、グループ鍵もセンター側および端末側で管理する必要がある。さらに、第２の従来例であっても第１の従来例と同様、端末の数が多くなるとセンターの暗号化、およびデータの送信の負担は大きくなり、また全局更新までの業務停止期間が長くなる。

【０００７】

【発明が解決しようとする課題】例えば１０００個の端末から１個の端末を排除して、残りの９９９個の端末で新たな共通の秘密鍵を共有する場合を考える。このとき、第１の従来例では９９９回の暗号化の処理と９９９回の暗号文の送信を行う必要がある。また第２の従来例で例えば１０００個の端末を５００個づつの２つにグループに分けた場合には、排除すべき端末を含むグループでは各端末ごとに４９９回、もう１方のグループにはグループ鍵で一括で、合計５００回の暗号化の処理と暗号文の送信が必要である。いずれにしても、センター側にとってこれら作業は非常に負担なものとなる。また、全局更新までの業務停止期間が長くなる。

【０００８】さらに、第２の従来例ではセンター側および端末側では、各端末の固有鍵とともに、グループ化の方法によっては多くのグループ鍵を管理する必要がある。

【０００９】本発明はかかる点に鑑み、特定の端末だけを排除して、他の端末で分配鍵情報を共有する方法であって、次の点を特徴とする鍵共有方法を実現することを目的とする。

【００１０】(1) センターから端末への通信量が少ない。センターにおける暗号処理の手間が少なく、暗号文の送信量が少ない。全局更新までの業務停止期間が短い。

【００１１】(2) 端末の秘密鍵が少ない。センターにおいて管理を行う端末の鍵が少ない。端末において管理を行う鍵が少ない。

【００１２】

【課題を解決するための手段】本発明の第１の構成における鍵共有装置は、センターと相異なる分配鍵情報を持つ複数の端末からなり、センターは全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、kを正整数とするとき、特定のk個の端末の分配鍵情報を同報で全端末に通知する通知部を備え、各端末は、分配鍵情報を格納する分配鍵情報格納部と、前記センターから通知されたk個の分配鍵情報を受信する受信部と、前記受信部で受信したk個の分配鍵情報と、前記分配鍵情報格納部に格納される分配鍵情報の計k+1個の分配鍵情報がすべて相異なる場合にのみ、これらk+1個の分配鍵情報より前記特定のk個の端末を除く残りの端末で共通の秘密鍵を算出する秘密鍵算出部からなり、前記各端末の分配鍵情報は、前記秘密鍵算出部に入力されるk+1個の分配鍵情報がすべて相異なる場合にのみ前記秘密鍵が復元できるように予め定められ各端末に分配されたものであることを特徴とする。

【００１３】本発明の第２の構成における鍵共有装置は、第１の構成における前記センターが、全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、前記全端末の分配鍵情報以外の予備の分配鍵情報を格納する予備分配鍵情報格納部と、kとmをそれぞれ正整数とするとき、特定のm個の端末の分配鍵情報と任意のk-m個の予備分配鍵情報の合計k個の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする。

【００１４】本発明の第３の構成における鍵共有装置は、第１の構成における前記センターが、前記全端末の分配鍵情報以外の予備の分配鍵情報を格納する予備分配鍵情報格納部と、任意のk個の予備の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする。

【００１５】本発明の第４の構成における鍵共有装置は、第１の構成における前記各端末は相異なる識別情報を保持し、前記センターは全端末分配鍵情報格納部の代

わりに、前記秘密鍵を保持する秘密鍵格納部と、前記秘密鍵と任意の端末の識別情報を入力として、対応する端末の分配鍵情報を算出する分配鍵情報算出部を備えていることを特徴とする。

【００１６】本発明の第５の構成における鍵共有装置は、第２、３の構成における前記各端末は相異なる識別情報を保持し、前記センターは前記予備分配鍵情報格納部の代わりに、前記秘密鍵を保持する秘密鍵格納部と、どの端末の識別情報とも異なる予備の情報と前記秘密鍵を入力として、前記予備の分配鍵情報を算出する予備分配鍵情報算出部を備えていることを特徴とする。

【００１７】本発明の第６の構成における鍵共有装置は、センターと相異なる分配鍵情報を持つ複数の端末からなり、センターは全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、kを正整数とするとき、特定のk個の端末の分配鍵情報を同報で全端末に通知する通知部を備え、各端末は、分配鍵情報を格納する分配鍵情報格納部と、前記センターから通知されたk個の分配鍵情報を受信する受信部と、前記受信部で受信したk個の分配鍵情報と、前記分配鍵情報格納部に格納される分配鍵情報の計k+1個の分配鍵情報がすべて相異なる場合にのみ、これらk+1個の分配鍵情報より前記特定のk個の端末を除く残りの端末で共通の第１の秘密鍵を算出する秘密鍵算出部と、前記第１の秘密鍵を全端末共通の変換方法で変換して第２の秘密鍵を求める変換部と、前記第２の秘密鍵から端末の新しい分配鍵情報を算出し、前記分配鍵情報格納部に格納して分配鍵情報を更新する分配鍵情報更新部からなり、前記各端末の更新前の分配鍵情報は、前記秘密鍵算出部において入力されるk+1個の分配鍵情報がすべて相異なる場合にのみ前記第１の秘密鍵が復元できるように予め定められ各端末に分配されたものであり、前記分配鍵情報更新部によって更新された各端末の分配鍵情報は、前記と同様前記第２の秘密鍵が復元できるように定めて各端末に分配されたものになり、前記各端末の変換部と分配鍵情報更新部は、外部より観察したり、変更できないものであり、前記センターの全端末分配鍵情報格納部は、前記各端末で更新された分配鍵情報を格納することを特徴とする。

【００１８】本発明の第７の構成における鍵共有装置は、第６の構成における前記変換部と分配鍵情報更新部を外部より観察したり、変更できない領域に備える代わりに、分配鍵情報更新部が、分配鍵情報を更新した後に前記第２の秘密鍵を消去することを特徴とする。

【００１９】本発明の第８の構成における鍵共有装置は、第６の構成における前記センターが、全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、前記全端末の分配鍵情報以外の予備の分配鍵情報を格納する予備分配鍵情報格納部と、kとmをそれぞれ正整数とするとき、特定のm個の端末の分配鍵情報と任意のk-m個の予備分配鍵情報の合計k個の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする。

【００２０】本発明の第９の構成における鍵共有装置は、第６の構成における前記センターが、前記全端末の分配鍵情報以外の予備の分配鍵情報を格納する予備分配鍵情報格納部と、任意のk個の予備の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする。

【００２１】本発明の第１０の構成における鍵共有装置は、第６の構成における前記センターは前記全端末分配鍵情報格納部の代わりに、前記第１の秘密鍵を保持する秘密鍵格納部と、前記第１の秘密鍵と任意の端末の識別情報を入力として、対応する端末の分配鍵情報を算出する分配鍵情報算出部と、前記第１の秘密鍵を各端末の変換部と同じ変換方法で変換して第２の秘密鍵を求め、前記秘密鍵格納部に格納して第１の秘密鍵を更新するセンター側変換部を備えることを特徴とする。

【００２２】本発明の第１１の構成における鍵共有装置は、第８、９の構成における前記センターは前記予備分配鍵情報格納部の代わりに、前記第１の秘密鍵を保持する秘密鍵格納部と、どの端末の識別情報とも異なる予備の情報と前記第１の秘密鍵を入力として、前記予備の分配鍵情報を算出する予備分配鍵情報算出部と、前記第１の秘密鍵を各端末の変換部と同じ変換方法で変換して第２の秘密鍵を求め、前記秘密鍵格納部に格納して第１の秘密鍵を更新するセンター側変換部を備えることを特徴とする。

【００２３】本発明の第１２の構成における鍵共有装置は、第６～１１の構成における前記各端末内の変換部およびセンター側変換部において、固定の変換の代わりに、外部から変更できる変換を用いることを特徴とする。

【００２４】本発明の第１３の構成における鍵共有装置は、第６～１１の構成における前記各端末内の分配鍵情報更新部で、前記第２の秘密鍵と前記端末の識別情報を用いて、前記端末の新しい分配鍵情報を算出することを特徴とする。

【００２５】本発明の第１４の構成における鍵共有装置は、第６～９の構成における前記各端末内の分配鍵情報更新部で、前記第２の秘密鍵と端末の更新前の分配鍵情報を用いて、前記端末の新しい分配鍵情報を算出することを特徴とする。

【００２６】本発明の第１５の構成における鍵共有装置は、センターと相異なる識別情報と分配鍵情報を持つ複数の端末からなり、kを正整数、pを素数とし、ak,ak-1,…,a1,a0をp未満の非負整数とするとき、識別情報IDiが与えられている端末の前記分配鍵情報は、法p上のk次多項式（数１）の座標(IDi,f(IDi))であり、前記センターは全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、特定のk個の端末の分配鍵情報を同報で全端末に通知する通知部を備え、各端末は、分配鍵情報を格納する分配鍵情報格納部と、前記センターから通知されたk

個の分配鍵情報を受信する受信部と、前記受信部で受信したk個の分配鍵情報と、前記分配鍵情報格納部に格納される分配鍵情報の計k+1個の分散鍵情報がすべて相異なる場合にのみ、これらk+1個の分配鍵情報である前記k次多項式の相異なるk+1個の座標から、前記k次多項式の１つ以上の係数を求めてそれらから秘密鍵を算出する秘密鍵算出部からなる。

【００２７】本発明の第１６の構成における鍵共有装置は、第１５の構成における前記センターが、全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、どの端末の識別情報とも異なる情報Xをx座標とする前記k次多項式の座標(X, f(X))を予備の分配鍵情報として格納する予備分配鍵情報格納部と、kとmをそれぞれ正整数とするとき、特定のm個の端末の分配鍵情報と任意のk-m個の予備分配鍵情報の合計k個の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする。

【００２８】本発明の第１７の構成における鍵共有装置は、第１５の構成における前記センターが、どの端末の識別情報とも異なる情報Xをx座標とする前記k次多項式の座標(X, f(X))を予備の分配鍵情報として格納する予備分配鍵情報格納部と、任意のk個の予備の分配鍵情報を同報で全端末に通知する通知部を備えることを特徴とする。

【００２９】本発明の第１８の構成における鍵共有装置は、第１５～１７の構成における前記センターは前記全端末分配鍵情報格納部または予備分配鍵情報格納部の代わりに、前記法p上のk次多項式を保持し、前記識別情報IDiが与えられている端末の分配鍵情報を、前記k次多項式に前記端末の識別情報を代入して求め、またどの端末の識別情報とも異なる情報を前記k次多項式に代入して前記予備分配鍵情報を求める分配鍵情報算出部を備えていることを特徴とする。

【００３０】本発明の第１９の構成における鍵共有装置は、センターと相異なる識別情報と分配鍵情報を持つ複数の端末からなり、kを正整数、pを素数とし、ak,ak-1,…,a1,a0をp未満の非負整数とするとき、識別情報IDiが与えられている端末の前記分配鍵情報は、法p上の第１のk次多項式（数１）の座標(IDi,f(IDi))であり、前記センターは全端末の分配鍵情報を格納する全端末分配鍵情報格納部と、特定のk個の端末の分配鍵情報を同報で全端末に通知する通知部を備え、各端末は、分配鍵情報を格納する分配鍵情報格納部と、前記センターから通知されたk個の分配鍵情報を受信する受信部と、前記受信部で受信したk個の分配鍵情報と、前記分配鍵情報格納部に格納される分配鍵情報の計k+1の分配鍵情報がすべて相異なる場合にのみ、これらk+1個の分配鍵情報である前記第１のk次多項式の相異なるk+1個の座標から、前記第１のk次多項式のk+1個の係数を求める秘密鍵算出部と、前記第１のk次多項式f(x)の各係数を変換して第２のk次多項式g(x)を求める変換部と、前記第２のk次多項式の座標（IDi, g(IDi)）を求めてこれを新たな分配鍵情報として、前記分配鍵情報格納部に格納する分配鍵情報更新部からなり、前記各端末の変換部と分配鍵情報更新部は、外部より観察したり、変更できないものであり、前記センターの全端末分配鍵情報格納部では前記各端末で更新された分配鍵情報を格納することを特徴とする。

【００３１】本発明の第２０の構成における鍵共有装置は、第１９の構成における前記各端末の変換部と分配鍵情報更新部を外部より観察したり、変更できない領域に備える代わりに、分配鍵情報更新部が、分配鍵情報を更新した後に前記第２のk次多項式g(x)の各係数を消去することを特徴とする。

【００３２】本発明の第２１の構成における鍵共有装置は、第１９の構成における前記端末の変換部で、前記端末の識別情報を変換してその結果を新たな識別情報とし、前記分配鍵情報更新部ではこの新たな識別情報をx座標とする前記第２のk次多項式の座標を求めてこれを新たな分配鍵情報とすることを特徴とする。

【００３３】本発明の第２２の構成における鍵共有装置は、第１９の構成における前記センターは前記全端末分配鍵情報格納部の代わりに、前記第１のk次多項式を保持し、前記識別情報IDiが与えられている端末の分配鍵情報を、前記第１のk次多項式に前記端末の識別情報を代入して求める分配鍵情報算出部と、前記第１のk次多項式f(x)のk+1個の係数を前記端末における変換部と同じ変換方法で変換して第２のk次多項式g(x)を求め、前記第１のk次多項式に置き換えてこれを保持するセンター側変換部を備えることを特徴とする。

【００３４】本発明の第２３の構成における鍵共有装置は、第１５～２２の構成におけるmを正整数とし、jを1からmのそれぞれの値をとるとき、jを添字とする各pjを素数としてこれに対応して前記と同様に法pj上のk次多項式fj(x)をそれぞれ定め、識別情報IDiが与えられている端末の分配鍵情報を、各座標(IDi,f1(IDi))(IDi,f2(IDi)),…, (IDi,fm(IDi))で与えられるm個の情報とし、センターにおける通知部では、特定のk個の端末の各m個の分配鍵情報を同報で全端末に通知し、各端末における秘密鍵算出部では、jを1からmのそれぞれの値をとるとき、各jについて相異なるk+1個の分配鍵情報がそろった場合にのみ、これらk+1個の分配鍵情報である前記k次多項式fj(x)の相異なるk+1個の座標から前記k次多項式fjのk+1個の係数を求めることを特徴とする。

【００３５】本発明の第２４の構成における鍵共有装置は、第１５～２２の構成におけるセンターと相異なる識別情報を持つ複数の端末からなり、k,mを正整数、jを1からmまでのそれぞれの値をとるとき、jを添字とする各pjを素数とし、aj,bjをpj未満の非負整数とするとき、識別情報IDiが与えられている端末の分配鍵情報を、法pj上の1次多項式（数２）の各座標(IDi,f1(IDi))(IDi,f2

(IDi)),…,(IDi,fm(IDi))で与えられるm個の情報とし、センターにおける通知部では、特定の端末の保持する各m個の分配鍵情報から任意に選んで同報で全端末に通知し、各端末は、前記センターから通知された分配鍵情報を受信する受信部と、前記j番目の分配鍵情報を格納する合計m個の分配鍵情報格納部と、前記受信部で受信した分配鍵情報の中から前記jに対応した分配鍵情報を選び、これと前記j番目の分配鍵情報格納部に格納された分配鍵情報と合わせて相異なる2個の分配鍵情報がそろった場合にのみ相異なる2個の座標から前記1次多項式fj(x)の係数を求める、合計m個の秘密鍵算出部を備える。

【００３６】本発明の第２５の構成における鍵共有装置は、第２４の構成における前記各jに対応するm個の多項式を、それぞれ1次以上の多項式とすることを特徴とする。

【００３７】本発明の第２６の構成における鍵共有装置は、第１５～２２の構成における前記素数pまたは素数pjを法とする多項式の代わりに、素体の拡大体上の多項式とすることを特徴とする。

【００３８】本発明の第２７の構成における鍵共有装置は、第１～２２の構成における前記秘密鍵算出部において、入力のk+1個の分配鍵情報に誤りが生じえる場合や、k+1個より多い分配鍵情報が入力された場合に、その中で正しいk+1個の相異なる分配鍵情報を用いて秘密鍵を算出することを特徴とする。

【００３９】本発明の第２８の構成における鍵共有装置は、第１５～２６の構成における前記各端末の秘密鍵算出部で求める多項式の係数の一部、または前記係数を含んだ計算結果を特定のk個の端末を除く各端末の共通鍵とすることを特徴とする。

【００４０】本発明の第２９の構成における鍵共有装置は、第２８の構成における前記センターは鍵データを発生し、これを前記共通鍵で暗号化した結果を、前記通信部で前記分配鍵情報とともに同報で全端末に通知し、前記特定のk個の端末を除く各端末では前記算出した共通鍵でこれを復号することを特徴とする。

【００４１】本発明の第３０の構成における鍵共有装置は、第１～２６の構成における前記秘密鍵にバージョン番号を付加し、センターは各バージョンの予備の分配鍵情報を保管し、バージョンが一致していない端末に前記必要な分配鍵情報を通知することを特徴とする。

【００４２】本発明の第３１の構成における鍵共有装置は、第６～１４、１９～２２の構成における前記秘密鍵にバージョン番号を付加し、バージョンが一致していない端末に正しいバージョンの秘密鍵を個別に暗号化して通知することを特徴とする。

【００４３】

【発明の実施の形態】本発明は、グループ内のある端末を排除して残りの端末で新しい秘密鍵を共有するという目的に、秘密分散法、または（k,n）しきい値法と呼ばれる公知の手法を、新たに適用したものである。秘密分散法や（k,n）しきい値法の説明は、例えば岡本栄司「暗号理論入門」共立出版（1993）の6.2節に詳しい。秘密分散法は秘密度の高い鍵の保管方法として従来より知られているものであり、例えば鍵を２つに分けて２人が保管し、使うときはその２人が集まらないと使えないといったものである。（k,n）しきい値法はこれを一般化し、秘密鍵をn個に分け（なお以下では秘密鍵を分けた結果のそれぞれを、分配鍵情報と称することにする）、n個の中から任意のk個を集めれば元の秘密鍵が復元でき、k個より少なければ元の情報が全く得られないものである。

【００４４】この（k,n）しきい値法の多項式を用いた例を用いて、本発明の実施の形態を以下に示す。

【００４５】（実施の形態１）本発明ではセンターと複数の端末からなり、各端末は相異なる分配鍵情報を保持している。図１は実施の形態１における各端末の分配鍵情報を模式的に示した図である。この実施の形態では、pを素数、a,b,xを法pのもとでの剰余元とし、法p上の１次多項式f(x)=ax+b modpを考え、各端末の識別情報をx座標としたy座標値を各端末の分配鍵情報としている。例えばIDiを識別情報とする端末の分配鍵情報はf(IDi)、IDjを識別情報とする端末の分配鍵情報はf(IDj)である。これらがそれぞれの端末にあらかじめ配付されているとする。なおここで各端末の識別情報は0からp-1までの整数であるとしている。また、１次多項式f(x)は素数pを法として求めるため、図１では表現されていないが、各端末の分配鍵情報は0からp-1までの整数値となる。ここで、各端末には１次多項式f(x)の１点の座標だけが分配鍵情報として配付されているため、２端末が結託しないかぎり自身の分配鍵情報から他の端末の分配鍵情報を類推することはできない。

【００４６】本実施の形態１においてはセンター側で各端末の識別情報と分配鍵情報を管理する。センターにおける管理では各端末の分配鍵情報そのものをデータベースで管理してもよいが、上記１次多項式f(x)だけを保管しておけば十分である。つまり、各端末の分配鍵情報はこの式に各端末の識別情報を代入すると、必要な都度求めることができる。

【００４７】ここまでの部分は（k,n）しきい値法における特にkが２である場合の秘密鍵の分散の方法と同じである。

【００４８】図２は、従来例と同様に５個の端末のうち端末T1だけを排除して残りの端末で共通の秘密鍵を共有する場合を示している。センターはまず、排除すべき端末T1の分配鍵情報を、保管している１次多項式に端末T1の識別情報を入力することにより求める。そして求めた端末T1の分配鍵情報を同報で各端末に送信する。例として図３に端末T3の内部構成を示している。１は端末T3の分配鍵情報f(ID3)の格納部であり、２はセンターから送

付された端末T1の分配鍵情報f(ID1)を受信する受信部、３は受信した分配鍵情報と格納している分配鍵情報f(ID3)を用いて、秘密鍵を求める秘密鍵算出部である。秘密鍵算出部では、図１において相異なる２つの座標点から対応する１次多項式の各係数、つまり傾きaや切片bを以下の（数３）を解いて求める。なお、以下の（数３）は法p上で計算する。

【００４９】

【数３】

$$a = (f(ID1)-f(ID3))/(ID1-ID3)$$

$$b = (ID1\times f(ID3)-ID3\times f(ID1))/(ID1-ID3)$$

【００５０】図では秘密鍵算出部は、端末T1を排除して残りの端末で共有する秘密鍵としてaを出力しているが、これは上記式を解いて求めた傾きa,bを用いてbまたはa+bを秘密鍵としてもよい。一方、端末T1も図３と同じ構成であるが、端末T1の秘密鍵算出部だけは自分の保持している分配鍵情報とセンターから配付された分配鍵情報が同じf(ID1)であるため、図１において１点の座標しか獲得していないことになり、前記１次多項式、つまり傾きaおよび切片bを双方とも決定することができない。従って上記秘密鍵を共有できない。

【００５１】ここでは簡単のために端末が全部で５つでありその中から端末T1だけを排除する場合について述べたが、同様にして任意の端末数の中から任意の１つの端末を排除することができる。従って、実施の形態１における鍵共有方式では、センターからわずか１回だけデータ送信することにより、任意の１個の端末を排除して残りの端末で秘密鍵を共有することができる。また、実施の形態１においては各端末はそれぞれ分配鍵情報を１つだけ保管しておけばよい。

【００５２】（実施の形態２）次に、最初に端末T1を排除し、続けて端末T2を排除する場合を考える。これは例えば５端末で共通の秘密鍵を共有してグループ内の暗号通信を行っている際に、まず端末T1が盗難され、これに対応して残りの４端末で新たな共通の秘密鍵を共有する、次にさらに端末T2も盗難される、といったシナリオである。

【００５３】実施の形態１では各端末は１つの１次多項式f(x)に対応した分配鍵情報を保持していた。本実施の形態ではこれに加えて、独立なもう１つの１次多項式g(x)=cx+d modp2に対応する分配鍵情報g(IDi)もあらかじめ各端末に蓄えておく。これは、端末T1を排除した段階でf(x)に関するすべての情報が公開されてしまうため、端末T2を排除するためには新たな多項式g(x)に対応した分配鍵情報が必要であるためである。

【００５４】ところで、この時の端末T2の排除の仕方として２つの場合が考えられる。１つ目は端末T2を排除するとき、端末T1は正規端末として復活し、T2を除いた残りの４端末で新たな秘密鍵を共有する場合である。２つ目は端末T2を排除するとき、その前に排除した端末T1も継続して排除し、T1,T2を除いた残りの３端末で新たな秘密鍵を共有する場合である。前者の場合には、端末T2を排除するためにg(ID2)を同報送信し、秘密鍵を係数c,dを用いて求めればよい。端末T1も含め端末T2以外の端末では、g(x)の係数c,dを求めることができる。一方端末T2だけは、g(x)を決定できないため、秘密鍵を求めることができない。次に、後者の場合について説明する。この場合秘密鍵を、f(x)の係数a,bとg(x)の係数c,dの双方を用いて求めればよい。また、f(x)の係数a,bの代わりに当初端末T1を排除して残りの端末で共有した前の秘密鍵を用いてもよい。端末T3～T5は上記a,b,c,dのいずれも算出でき新たな秘密鍵を求められる。一方、端末T1はf(x)の係数a,bを求められず、端末T2はg(x)の係数c,dを求められないため、双方を排除することができる。

【００５５】なお、以上の実施の形態２では端末排除の回数が２回（最初にT1、次にT2を排除）であったが、これに引き続いてさらに端末を排除するためには、排除の回数に応じた分配鍵情報をあらかじめ各端末に格納しておく必要がある。先にも述べたとおり、これは前の端末排除に用いた分配鍵情報が次の端末排除のために利用できないためである。

【００５６】（実施の形態３）実施の形態２では、あらかじめ端末排除の回数分の多項式を選択し、これに対応した分配鍵情報を各端末に格納しておく。そして端末排除のたびにこれを順番に使用し、その都度排除した端末以外で、新しい秘密鍵が共有されるものであった。これに対し、実施の形態３では、１つの分配鍵情報を格納し、端末排除のたびにこれを更新して新しい分配鍵情報を各端末で求めるといった方法である。実施の形態２に比べて端末における分配鍵情報の格納領域が削減できる。また実施の形態２が端末排除の回数があらかじめ格納している分配鍵情報の個数に依存して有限であったのに対し、実施の形態３ではこの制限がない。図４は、端末T3の構成を示したものであり、図３に分配鍵情報を更新する部分を追加している。１、２、３は図３と同じである。端末T3は秘密鍵算出部３の出力として前記１次多項式f(x)の傾きaと切片bを求める。なお、図では秘密鍵算出部は、端末T1を排除して残りの端末で共有する秘密鍵としてaを出力しているが、これは上記求めた傾きa,bを用いて例えばbまたはa+bなどを秘密鍵としてもよい。４は秘密鍵算出部２で求めた前記aとbをそれぞれ固定の秘密変換して、その結果のa'、b'を新たな傾きと切片とする新しい１次多項式f'(x)=a'x+b' modpを求める変換部である。５はこの新しい１次多項式f'(x)に、端末T3の識別情報格納部５に格納されているID3を代入して新しい分配鍵情報を求める分配鍵情報更新部である。この出力が１の分配鍵情報格納部に新たに設定され、分配鍵情報が更新される。なお、このうち変換部と分配鍵情報更新部はユーザに内部が見られないことが必要である。図４におけるハッチングはこのことを意味にしている。

これは、もし端末で新しい多項式f'(x)が見られると、他の端末の分配鍵情報は勿論、本来センターから排除すべき端末の分配鍵情報が通知されて初めて求められるはずの秘密鍵がすでに求められるからである。なお、変換部と分配鍵情報更新部をユーザに見られない部分で実行する代わりに、実行時のデータを見ることはできないという前提のもと、分配鍵情報を更新した後に新しい多項式f'(x)の係数a', b'を消去してもよい。これにより、ユーザに見られない特別な部分を備える必要はなくなる。

【００５７】なお、この場合センター側でも同じ変換を行って前のf(x)を新しい１次多項式f'(x)に更新する。そして、この後さらに端末T2を排除する場合には、センターは新しい１次多項式f'(x)から端末T2の分配鍵情報f'(ID2)を獲得してこれを同報で端末に通知する。排除されていない端末T3では分配鍵情報格納部に格納された分配鍵情報f'(ID3)とセンターから送られた情報f'(ID2)を用いて１次多項式f'(x)の係数a',b'を求めこれらから新しい秘密鍵を算出する。一方、端末T2は格納している分配鍵情報とセンターからの分配鍵情報が重なるため前記１次多項式f'(x)を決定できない。また最初に排除された端末T1も、最初の１次多項式f(x)の係数a,bを獲得できないために、新しい１次多項式f'(x)の係数a'b'を獲得できない。そのため端末T2が排除された場合には継続して端末T1も排除されている。

【００５８】以上端末排除回数が２回の場合について述べたが、３回以上の場合も同様で、秘密鍵算出部において求める多項式の係数を順次変換して、次の多項式を求め新たな分配鍵情報を求める。従ってこの場合端末排除回数が何回であっても、各端末で保有する分配鍵情報は１つであり、またセンターにおける管理もそのときの１次多項式だけである。

【００５９】以上、ここまでの実施の形態１～３では、１回には１個の端末だけを排除する場合について述べたが、以降の実施の形態４および５では、同時に複数の端末を排除する方法について述べる。

【００６０】（実施の形態４）図５は実施の形態４における各端末の分配鍵情報を模式的に示した図である。この例では、素数pを法としてその上での２次多項式F(x)=ax２+bx+c modpを考え、各端末の識別情報をx座標としたy座標値を各端末の分配鍵情報としている。例えばIDiを識別情報として持つ端末の分配鍵情報は、F(IDi)となり、これらが各端末にあらかじめ配付されているとする。端末の分配鍵情報は、F(x)が素数pを法としているため、図５では表現されていないが0からp-1までの整数値となる。センター側では各端末の分配鍵情報と識別情報を管理する。管理方法としては分配鍵情報をそれぞれデータベースで保管してもいいが、上記２次多項式だけを保管し、各端末の識別情報を用いて必要な都度対応する端末の分配鍵情報を算出してもよい。

【００６１】図６は、５個の端末のうち端末T1と端末T2を同時に排除して残りの端末で秘密鍵を共有する場合を示している。センターはまず、排除すべき端末T1とT2の分配鍵情報を、保管している２次多項式にそれぞれの識別情報を入力することにより求める。そして求めた分配鍵情報F(ID1), F(ID2)を同報で各端末に送信する。例として図７に端末T3の内部構成を示している。１１は端末T3の分配鍵情報F(ID3)の格納部であり、１２はこの分配鍵情報F(ID3)とセンターから送付された２つの端末の分配鍵情報F(ID1),F(ID2)を用いて、秘密鍵を求める秘密鍵算出部である。秘密鍵算出部では、図５において相異なる３点の座標点F(ID1),F(ID2),F(ID3)から対応する２次多項式の係数a,b,cを求め、これをもとに秘密鍵を算出する。なお、a,b,cを求めるための具体的な計算は以下の（数４）のとおりである。なお、以下の（数４）は法p上で計算する。

【００６２】

【数４】

$$x12 = ID1 - ID2,$$

$$x23 = ID2 - ID3,$$

$$x13 = ID1 - ID3,$$

$$x123 = x12 \times x23 \times x13,$$

$$a = (1/x123) \times (x23 \times F(ID1) - x13 \times F(ID2) + x12 \times F(ID3))$$

$$b = (1/x123) \times (-(ID2+ID3) \times x23 \times F(ID1) + (ID1+ID3) \times x13 \times F(ID2) - (ID1+ID2) \times x12 \times F(ID3))$$

$$c = (1/x123) \times (ID2 \times ID3 \times x23 \times F(ID1) - ID1 \times ID3 \times x13 \times F(ID2) + ID1 \times ID2 \times x12 \times F(ID3))$$

【００６３】端末T4,T5も同様に係数a,b,cを求めて端末T3と同じ秘密鍵を算出する。図７ではaを秘密鍵としているが、これが例えばaやa+b、a+b-cなどであってよい。一方、端末T1,T2も図７と同じ構成であるが、端末T1と端末T2の秘密鍵算出部は自分の保持している分配鍵情報とセンターから配付された分配鍵情報が重なっているため、図５において２点の座標しか獲得していないことになり、前記２次多項式を決定できない。

【００６４】このことにより、第１の実施の形態における鍵共有方式では、センターから２個のデータを送信す

ることにより、同時に２個の端末を排除して残りの端末で秘密鍵を共有できる。

【００６５】実施の形態４は２端末を同時に排除するが、１端末だけを排除することも可能である。そのためにはセンターは予備の分配鍵情報を求める。つまり、図５のグラフにおけるx座標において各端末の識別情報に割り当てていない値をいくつか予備に確保しておく。そして対応する座標点を予備の分配鍵情報とする。この分配鍵情報はあらかじめデータベースで保管しておいても良いし、多項式だけを保管しておいて分配鍵情報は都度求めてもよい。例えばセンターが端末T1だけを排除する場合には、端末T1の分配鍵情報と予備の分配鍵情報のうち任意の１つを同報で通知する。端末T1以外の端末では、自身の分配鍵情報とセンターから送付される端末T1の分配鍵情報と予備の情報を用いて秘密鍵を求める。端末T1だけは自身の分配鍵情報とセンターから送付される一方の情報が重なっているため秘密鍵を求めることができない。

【００６６】また、上記述べた予備の分配鍵情報を用いることにより、どの端末も排除せずに秘密鍵の更新だけを行うことも可能である。つまり、実施の形態４の例ではセンターから端末に同報で通知する２つの情報を双方とも予備の分配鍵情報とする。このことにより、すべての端末は新しい秘密鍵を算出できる。この場合、端末側は秘密鍵の定期的な更新なのか、端末を排除するための更新なのかを全く意識せず、同じ処理を行うだけでよい。

【００６７】なお、以上の実施の形態４においては２個までの端末を同時に排除するために２次多項式を用いたが、一般にN個までの端末を排除するためにはN次多項式を用いる。このとき、センターから端末に同報通信されるデータの個数はN個である。

【００６８】（実施の形態５）次に、複数端末を同時に排除するためのもう１つの方法を実施の形態５として説明する。図８は実施の形態５における各端末の分配鍵情報を模式的に示した図である。この例では、素数p1、p2を法としてその上での１次多項式を２つ（f(x)=ax+b mod p1、g(x)=cx+d modp2）考え、それぞれの多項式における各端末の識別情報をx座標としたy座標値を各端末の分配鍵情報としている。例えばIDiを識別情報として持つ端末の分配鍵情報は、f(IDi)とg(IDi)となり、これらが各端末にあらかじめ配付されているとする。なお、前者を端末の第１の分配鍵情報、後者を第２の分配鍵情報と呼ぶことにする。センター側では上記１次多項式f(x),g(x)を保管している。

【００６９】図９は、実施の形態４と同様に５個の端末のうち端末T1と端末T2を同時に排除して残りの端末で秘密鍵を共有する場合を示している。センターはまず、保管している１次多項式f(x),g(x)に対応する端末の識別情報を入力することにより、端末１の第１の分配鍵情報f(ID1)と端末２の第２の分配鍵情報g(ID2)を求める。そして求めた分配鍵情報を同報で各端末に送信する。例として図１０に端末T3の内部構成を示している。２１は端末T3の第１の分配鍵情報f(ID3)の格納部であり、２２はこの分配鍵情報f(ID3)とセンターから送付された端末T1の分配鍵情報f(ID1)を用いて、１次多項式f(x)に関する中間秘密鍵を求める第１の中間秘密鍵算出部である。また２３は端末T3の第２の分配鍵情報g(ID3)の格納部であり、２４はこの分配鍵情報g(ID3)とセンターから送付された端末T2の分配鍵情報g(ID2)を用いて、１次多項式g(x)に関する中間秘密鍵を求める第２の中間秘密鍵算出部である。そして２５は前記第１、第２の中間秘密鍵を用いて秘密鍵を算出する秘密鍵算出部である。前記第１、第２の中間秘密鍵算出部では、図８における直線f(x)およびg(x)上の相異なる２点から直線の係数（傾き、切片）の全部または一部から所定の方法で導出されるデータを中間秘密鍵として求める。図ではそれぞれの傾きの係数a,cを出力する場合について示している。前記秘密鍵算出部では前記中間秘密鍵算出部の出力を、ある関数Data()に入力し秘密鍵を算出する。秘密の関数としては例えば入力値の加算や排他的論理和といった簡単なものであってもよい。図１０では中間秘密鍵a,cの加算結果a+cを秘密鍵としている。

【００７０】ところで、端末１は第１の中間秘密鍵を得ることができない。また端末２は第２の中間秘密鍵を得ることはできない。この結果、端末１および２は他の端末が共有する秘密鍵を獲得することができない。

【００７１】なお、この例ではセンターはf(ID1)とg(ID2)を全端末に同報で配送して端末１と端末２を排除したが、この代わりにg(ID1)とf(ID2)を配送してもよい。

【００７２】この実施の形態５では、実施の形態４が２次多項式を用いて実現していることを１次多項式を２つ用いて実現している。実施の形態４では、秘密鍵算出部において３個の座標から２次多項式を解くことが必要であり、そのためには（数４）で示した比較的複雑な計算を行なわなければならない。これに対して実施の形態５では各中間秘密鍵では１次多項式を解けばよく（（数３）の計算）、トータルでは実施の形態４に比べて計算量が削減できる。具体的には（数３）の計算には乗算が2回、除算が1回（加減算は乗除算の計算量に比べると無視できるほどわずかであるため、ここでは考慮しない）かかり、（数４）の計算には乗算が23回、除算が1回かかる。そのため、実施の形態５では実施の形態４に比べてはるかに乗算回数が少なくてすむ。

【００７３】なお、実施の形態５においても１端末だけを排除することが可能である。方法としては３つある。第１の方法は、例えばf(x)の方だけを使用する。このとき図１０においては第１の中間秘密鍵算出部の出力が秘密鍵となる。第２の方法は、例えばf(x)において排除すべき端末の分配鍵情報を送付し、g(x)においては予備の

分配鍵情報を送信する方法であってもよい。この場合すべての端末は第２の中間秘密鍵を獲得できるが、排除される端末だけは第１の中間秘密鍵を算出できないため、最終的な秘密鍵を求めることができない。第２の方法の場合には端末側は排除すべき端末の数が１端末だけなのか２端末なのかを意識することなく常に同じ処理を行えばよい。また、第３の方法では、端末T1だけを排除するに端末T1の２つの分配鍵情報f(ID1)とg(ID1)を送付する。端末T1以外の端末は２つの中間共通データを求めこれから秘密鍵を算出できる。端末T1だけは中間共通データを双方とも算出することができない。

【００７４】なお、前記第３の方法を、実施の形態１を改善して端末における秘密鍵算出の計算量を削減する方法と見ることができる。実施の形態１に述べた方法では、秘密情報は0以上p-1以下の整数となり、この総当たり攻撃に対する安全性を確保するためにはpを大きく取る必要がある。ところが法pを大きくすると秘密鍵の算出のための計算がすべて大きな法の計算となり計算量が多くなる。その計算量の増加はpの大きさに比べて指数関数的に増加する。例えばpを32ビットの値として32ビットの幅の乗算の計算量は、16ビット幅の乗算の計算量の4倍になるといった具合である。そこで、この計算量を削減するため、大きな法pの代わりに比較的小さな法p'を複数備え、この上での１次多項式を考える。各端末は、それぞれの１次多項式に対応する座標を分配鍵情報として保持する。センターは排除する端末の、複数の分配鍵情報を同報で通知し、各端末ではそれぞれから中間秘密鍵を求め、それらを結合することにより大きな法p程度の秘密鍵を獲得する。これにより処理量の削減、速度アップが可能になる。

【００７５】なお、実施の形態５では２個の端末を同時に排除するために１次多項式を２個用いたが、一般にN個の端末を同時に排除するためには１次多項式をN個用いればよい。また、１次多項式ではなく比較的低次の多項式を複数個用いてもよい。

【００７６】なお、実施の形態４、５においても実施の形態３で述べている各端末の分配鍵情報の更新部分を追加することができる。

【００７７】以上の５つの実施の形態では各端末の分配鍵情報を、素体上の多項式の座標としていたが何もこれに限るものではない。例えばこれを素体の拡大体等の一般の有限体上の多項式の座標に拡張することができる。その他相異なるk+1個の分配鍵情報がそろった場合にのみ、各端末間で共通の鍵が共有できるものであればよい。この部分は秘密分散や（k,n）しきい値法に関する公知の技術が適用される。

【００７８】また、実施の形態３（図４）の変換部を、多項式の係数をそれぞれ固定の秘密変換して実現しているが、秘密鍵を固定に変換するようなものであればどんなものでもよい。この変換自身を外から変更できるようにしておいてもよい。

【００７９】また、実施の形態３の分配鍵情報更新部において、各端末の識別情報を元に分配鍵情報を算出しているが、更新前の分配鍵情報を元に新しい分配鍵情報を算出しても良い。ただし、この場合には分配鍵情報が各端末ごとに重ならないよう留意する必要がある。

【００８０】また、特に実施の形態２のように分配鍵情報を自動的に端末内で更新していく場合には、各端末が共有する秘密鍵は必ずしもセンターが都度指定したものにはならない。そこで、センターが秘密鍵Kを指定したい場合には、センターは前記Kを保持している秘密鍵で暗号化し、排除する端末の分配鍵情報などと同時に同報で各端末に送付する。各端末では秘密鍵算出部の出力を用いて、センターから送られてきたデータを復号し、その結果を秘密鍵とする。

【００８１】また、このように秘密鍵を同報で更新していく場合、何らかの都合でセンターからの通信を獲得できず、更新ができない端末が生じる場合がある。このために、各分配鍵情報にはバージョン番号を付加するとよい。そしてセンターとのやり取りでこのバージョンが食い違ってしまった場合には、センターに要求を行い、センターが保持している各バージョンの予備の分配鍵情報を順次送付してもらい、秘密鍵を最新のバージョンまで順番にバージョンアップすることができる。また、端末に分配鍵を更新する部分が備えられている場合には、センターはバージョン合わせが必要となる端末に対して、最新の秘密鍵を個別に暗号化して送ってもよい。当該の端末では最新の秘密鍵を他の端末と共有すると同時に、この秘密鍵から次の秘密鍵と分散鍵情報を算出する。なお、この場合のバージョン合わせの方法では、端末から端末が最初保持している秘密鍵のバージョンの情報を知る必要がないし、センターから１回通知するだけでバージョンが整合する。

【００８２】また、センターから端末に同報で通知される分配鍵情報が途中で誤りを含んでしまう場合がある。こういった場合の研究が秘密分散の分野でなされている。研究成果は、M.Tompa, and H.Woll, "How to Share a Secret with Cheaters", Journal of Cryptology, v.1, n.2, 1988, pp133-138などを参照。本発明はこのような研究成果もそのまま鍵共有方法に応用できる。

【００８３】

【発明の効果】以上説明したように、本発明では例えば１個の端末を排除して残りの端末で同じ秘密鍵を獲得するために、センターはわずか１個のデータを送付するだけでよい。一般にはN個以下の端末を同時に排除するためには、センターはN個の情報を送ればよい。このことによりセンター側の処理の手間および通信量が削減され、また端末間での秘密鍵の更新のずれが少ないため不都合が生じにくい。

【００８４】また、本発明の請求項４および５に対応し

た構成により、センター側では各端末の分配鍵情報をそれぞれ管理する必要はなく、実施の形態ではその元になる多項式だけを管理すればよい。そして必要な場合に多項式に端末の識別情報を代入することにより対応する端末の分配鍵情報を得ることができる。これによりセンター側の端末管理の負担が軽減される。

【００８５】また、本発明の請求項６に対応した構成により、分配鍵情報は変換部と分配鍵情報更新部を用いて更新することにより、各端末においては１つの分配鍵情報を管理しておけばよい。これにより端末側およびセンター側の分配鍵情報の管理負担が軽減される。

【００８６】また、本発明の請求項２３から２６に対応した構成により、高次の多項式を使用する代わりに、比較的低次の多項式を複数個用いることにより、安全性を保持しつつ端末における秘密鍵の算出のための計算量を削減することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１における各端末の分配鍵情報を模式的に示す図

【図２】本発明の実施の形態１においてセンターが５つの端末のうち端末T1を排除する場合について示す図

【図３】本発明の実施の形態１における端末T3の内部の構成を示す図

【図４】本発明の実施の形態３における端末内での分配鍵情報の更新を可能にする構成を示す図

【図５】本発明の実施の形態４における各端末の分配鍵情報を模式的に示す図

【図６】本発明の実施の形態４においてセンターが５つの端末のうち端末T1と端末T2を同時に排除する場合について示す図

【図７】本発明の実施の形態４における端末T3の内部の構成を示す図

【図８】本発明の実施の形態５における各端末の分配鍵情報を模式的に示す図

【図９】本発明の実施の形態５においてセンターが端末T1と端末T2を同時に排除する場合について示す図

【図１０】本発明の実施の形態５における端末T3の内部の構成を示す図

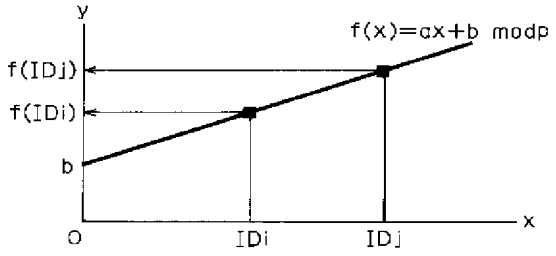
【図１１】従来例１の鍵共有方法の構成を示す図

【図１２】従来例２の鍵共有方法の構成を示す図

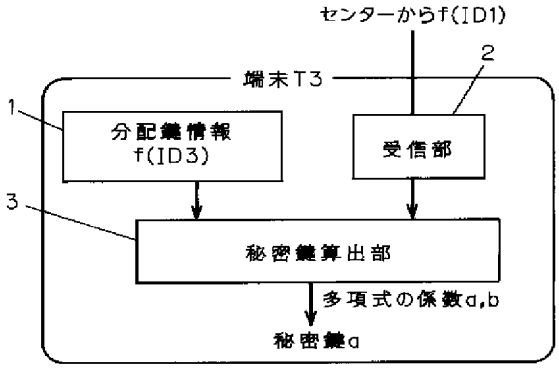
【符号の説明】

１　分配鍵情報格納部
２　受信部
３　秘密鍵算出部
４　変換部
５　分配鍵情報更新部
６　識別情報格納部
１１　分配鍵情報格納部
１２　受信部
１３　秘密鍵算出部
２１　分配鍵情報格納部
２２　中間秘密鍵算出部
２３　分配鍵情報格納部
２４　中間秘密鍵算出部
２５　秘密鍵算出部

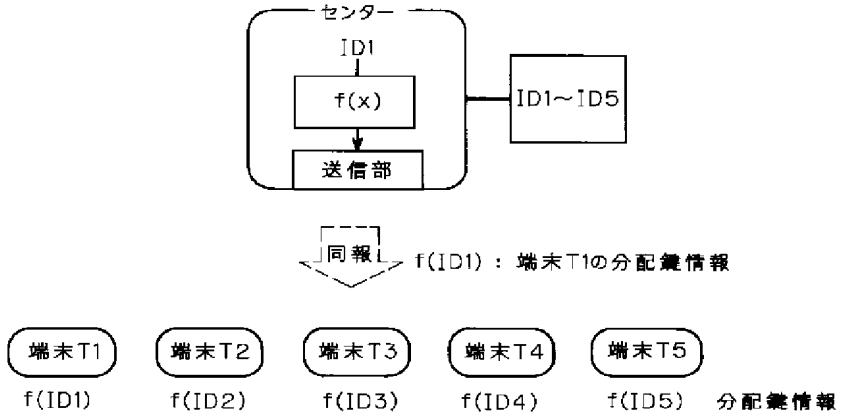
【図１】



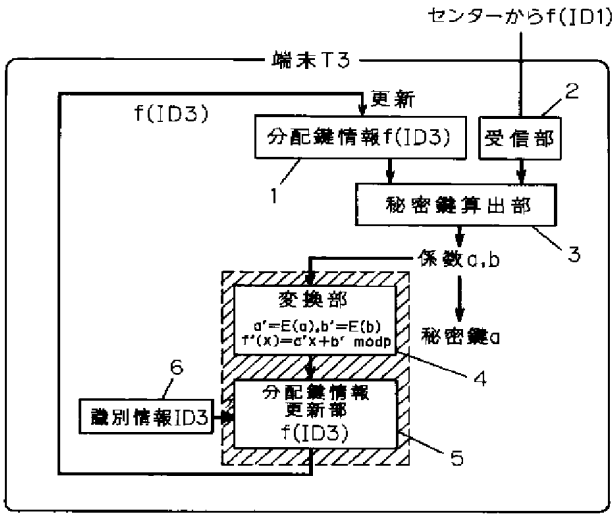
【図３】



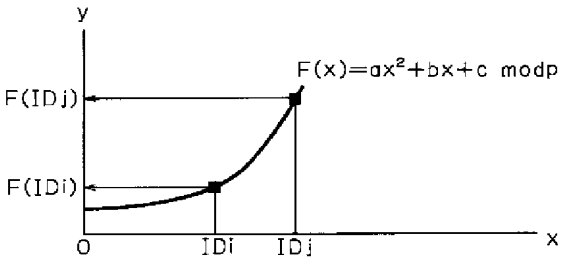
【図２】


センター
ID1
f(x)
送信部
ID1～ID5
同報
f(ID1)：端末T1の分配鍵情報
端末T1
端末T2
端末T3
端末T4
端末T5
f(ID1)
f(ID2)
f(ID3)
f(ID4)
f(ID5)
分配鍵情報

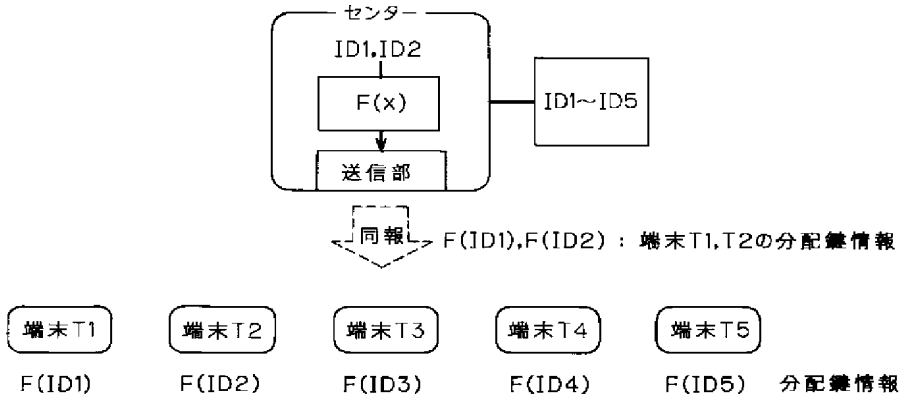
【図４】


センターからf(ID1)
端末T3
更新
f(ID3)
分配鍵情報f(ID3)
受信部
秘密鍵算出部
係数a,b
変換部
a'=E(a),b'=E(b)
f'(x)=a'x+b' modp
秘密鍵a
分配鍵情報
更新部
f(ID3)
識別情報ID3
1
2
3
4
5
6

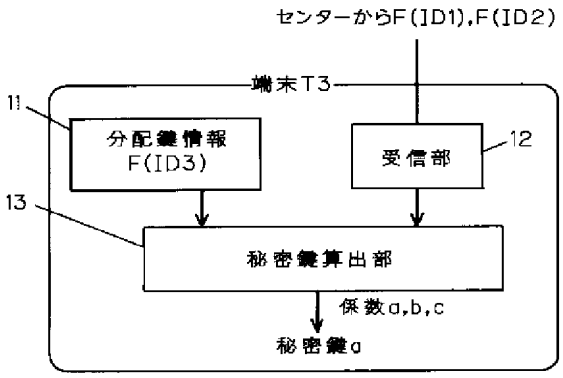
【図５】


y
F(x)=ax²+bx+c modp
F(IDj)
F(IDi)
0
IDi
IDj
x

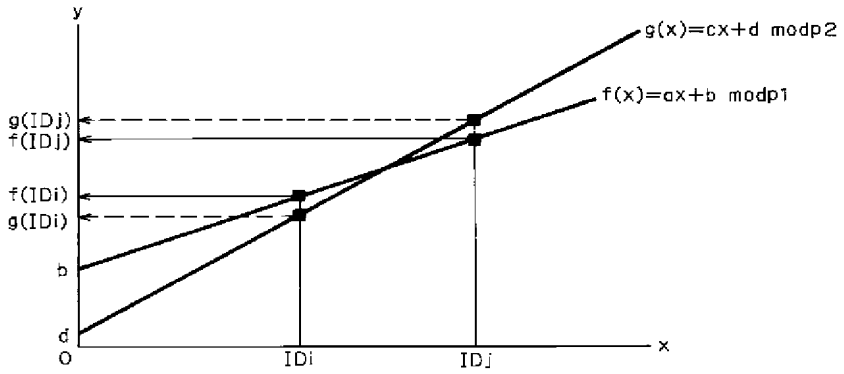
【図６】


センター
ID1,ID2
F(x)
送信部
ID1～ID5
同報
F(ID1),F(ID2)：端末T1,T2の分配鍵情報
端末T1
端末T2
端末T3
端末T4
端末T5
F(ID1)
F(ID2)
F(ID3)
F(ID4)
F(ID5)
分配鍵情報

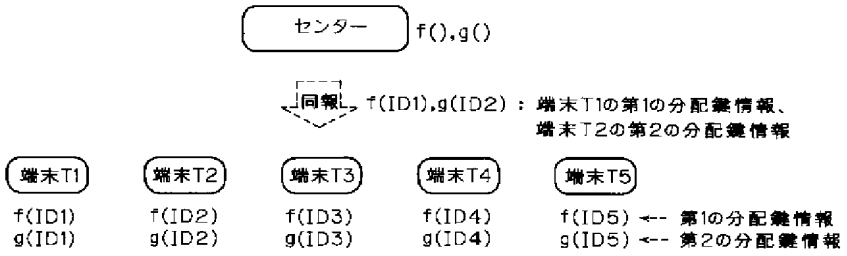
【図７】


センターからF(ID1),F(ID2)
端末T3
11
分配鍵情報
F(ID3)
受信部
12
13
秘密鍵算出部
係数a,b,c
秘密鍵a

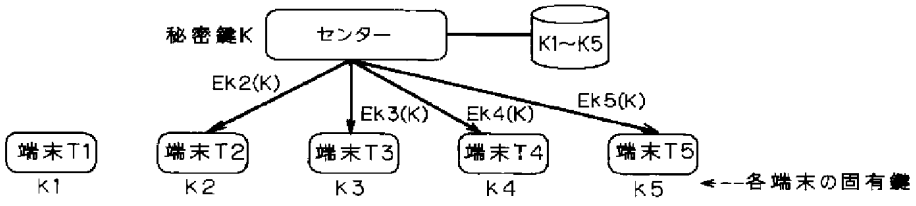
【図８】


y
g(x)=cx+d modp2
f(x)=ax+b modp1
g(IDj)
f(IDj)
f(IDi)
g(IDi)
b
d
O
IDi
IDj
x

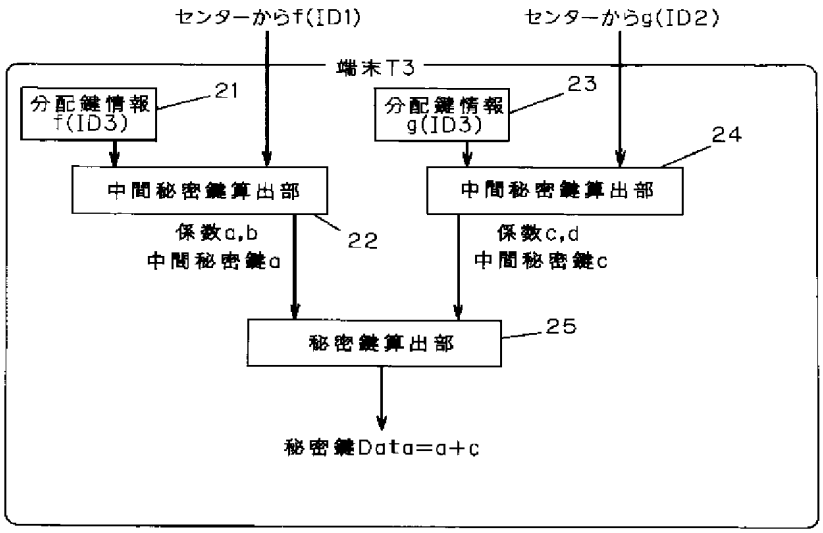
【図９】


センター
f(),g()
同報
f(ID1),g(ID2)：端末T1の第1の分配鍵情報、
端末T2の第2の分配鍵情報
端末T1
端末T2
端末T3
端末T4
端末T5
f(ID1)
g(ID1)
f(ID2)
g(ID2)
f(ID3)
g(ID3)
f(ID4)
g(ID4)
f(ID5) <-- 第1の分配鍵情報
g(ID5) <-- 第2の分配鍵情報

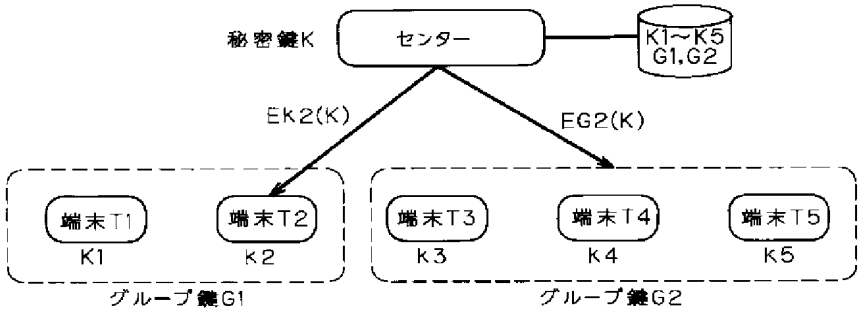
【図１１】


秘密鍵K
センター
K1~K5
Ek2(K)
Ek3(K)
Ek4(K)
Ek5(K)
端末T1
K1
端末T2
K2
端末T3
K3
端末T4
K4
端末T5
K5
<--各端末の固有鍵

【図１０】



【図１２】



フロントページの続き

(72)発明者　苫米地　明孝
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　神田　潤
大阪府門真市大字門真1006番地　松下電器産業株式会社内